

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA
Criminal No. 17-107-11 (DWF/TNL)

UNITED STATES OF AMERICA,

Plaintiff,

v.

BHUNNA WIN,
a/k/a Bhunna Siriangkunwanish,
a/k/a J'Yung,

Defendant.

**RESPONSE IN OPPOSITION
TO DEFENDANT'S SUPPRESSION
MOTION**

The United States of America, by and through its attorneys, Erica H. MacDonald, United States Attorney for the District of Minnesota, and Laura M. Provinzino and Melinda A. Williams, Assistant United States Attorneys, files this response in opposition to the defendant Bhunna Win's motion to suppress (Doc. No. 835).

I. FACTUAL AND PROCEDURAL BACKGROUND

On May 24, 2017, Bhunna Win was arrested and law enforcement executed a search warrant at her premises at 6xxx Red Deer Street in San Diego, California. The search warrant was signed by the Honorable Jan M. Adler and specifically authorized the search of computer related evidence, including passwords, encryption keys, and other access devices that may be necessary to access the computer, wireless telephone, or other electronic device or storage media.¹

¹ The search warrant has been disclosed to defense counsel. It is currently under seal in the Southern District of California, 17-mj-1433 (JMA), but will be provided to the Court.

During the nationwide operation, Bhunna Win was arrested at 6:20 a.m. A team of approximately 12 agents from Homeland Security Investigations (HSI) and the Internal Revenue Service – Criminal Investigations (IRS-CI) executed the arrest and search warrants. Numerous responsive items were seized during the search warrant.² Win was detained for a brief period of time in her home. During this time, an IRS-CI computer specialist asked for the password of a cell phone. Notably, the password Win provided did not work. Moreover, the vast majority of electronic devices seized pursuant to the search warrant, which the defendant does not challenge, were not password protected.

Shortly thereafter, Win was transported to HSI's headquarters for further processing and interview. Two agents and a senior investigator recorded a conversation with Win. The recording started at 7:51 a.m. and concluded at 8:07 a.m. The conversation was in English, during which Win answered a series of biographical questions, including her date of birth, use of aliases, immigration status, current employment, and information about her family, among other information. A Thai interpreter was available on a language line but was not needed as the defendant spoke fluent English. Then Win was advised of her rights

² These items included: (1) an Asus Digital Storm with s/n 13349707; (2) an Apple iPhone model A1332; (3) an MSI Laptop; (4) a "Mini" car thumb drive; (5) a Samsung phone model GT-E1200Y with s/n R21F62PCWEV; (6) a ZTE phone model Z432 with s/n 9B050821170B; (7) a BLU phone model A010U with s/n LS1546555312; (8) an Apple MacBook Air A1465 with s/n C02PP14QGFWL; (9) an Apple iPhone model A1784 with s/n F2LSF423HFYJ; (10) an Apple iPad model A1567 with s/n DMPNKAXGG5YR; (11) an Apple iPhone model A1634 with s/n C39QLBHGRXK; (12) an Oddo A33 Android phone; (13) a Microsoft Surface with s/n 006729450752; (14) a Verbatim external HD with s/n JA308Y060374; (15) a Kingston Wi-Drive with s/n JXS132302771; (16) an X-Media external HD with s/n EN225012110500; and (17) a Kingston 1 GB MicroSD; and (18) a Seagate Backup Plus with s/n NA7ERHCL. The inventory of items seized, which was part of the search warrant return, is attached as Exhibit 1.

through the U.S. Immigration and Customs Enforcement form that was in English and Thai. An agent read the form in English; Win was provided the written rights at the same time so she could follow along in both English and Thai. After being advised of her rights, Win elected not to speak to law enforcement stating: “I don’t want to speak today.” No questions were asked about computers or anything else related to the investigation.

Consent is not necessary here as law enforcement had authority to search the digital devices from the search warrant. The defendant seeks now to suppress evidence for which she provided voluntary consent both at the time the search warrant was executed, and, again, during a subsequent proffer session with the United States where she was represented by counsel. Win fails to mention this consent in her motion.

On December 6, 2017, with her counsel, Win flew in from California to meet with the case agents and undersigned AUSAs. During that two-day meeting, which was conducted in English, Win signed a consent to search form covering “all electronic devices seized by law enforcement on May 24, 2017, including cell phones, iPads, computer, etc., as detailed further in the search warrant return.” *See* Consent to Search attached hereto as Exhibit 2. The form advised Win that she could refuse to consent to the property being searched. Win was also informed that anything discovered during such a search may be used against her in court. Win authorized the search without threats, promises, pressure, or coercion of any kind. Win both printed her name and signed the consent to search form, which was witnessed by law enforcement and Win’s attorney at the time, Tom Dunnwald. Win additionally provided the passcode that opened an iPhone and iPad.

II. THE ARGUMENT

Regardless of how the defendant feels about the consent of a search, “the Fourth Amendment requires only that the police reasonably believe the search to be consensual.” *United States v. Zamora-Garcia*, 831 F.3d 979, 983 (8th Cir. 2016). In the instant case, a computer specialist with IRS-CI asked Win for the passcode to her phone as he was going through other, non-password protected, electronic devices.³ The computer specialist posed the question without any show of force or coercion.⁴ As is evident from the recording of the morning of her arrest, Win is an adult, understands English well enough to interact with law enforcement, was not intoxicated, and was clearly someone of at least average intelligence. Even persons who have been arrested and in custody can voluntarily consent to a search or to provide a passcode. *See United States v. Watson*, 423 U.S. 411, 424 (1976); *United States v. Saenz*, 474 F.3d 1132, 1137 (8th Cir. 2007) (finding that even though no *Miranda* warning was given until after the search was completed, this does not nullify an otherwise voluntary consent).

³ All of these devices were covered by the search warrant that was being executed.

⁴ A defendant’s cooperation is deemed involuntary (and thus inadmissible) if it “was extracted by threats, violence, or ... promises, such that the defendant's will was overborne and his capacity for self-determination critically impaired.” *United States v. Gallardo-Marquez*, 253 F.3d 1121, 1123 (8th Cir. 2001) (citations omitted). Such a determination is made based on a totality of the circumstances. *Id.* Simply put, there is no evidence that the police intended to “overbear” Win’s will. The computer specialist had no physical contact with her, and did nothing other than motion to the phone and request her password. In *Guallardo-Marquez*, the police were arguably more coercive, in that they did not allow the defendant to get dressed before arrest, and did not prevent the defendant’s young daughter from seeing him in a state of undress. *Id.* Despite these actions, the court still ruled that law enforcement’s actions did not warrant the exclusion of the defendant’s voluntary statements. *Id.* at 1123–24.

Even if we assume that the officer's actions were unconstitutional, Win's motion leaves out facts that are crucial to the analysis of whether evidence should be excluded. The Supreme Court has consistently ruled that if evidence would have been discovered regardless of an officer's unlawful actions, that evidence would be admissible. *See Utah v. Strieff*, 136 S.Ct. 2056 (2016); *Nix v. Williams*, 467 U.S. 431 (1984). It is true that initially, Win did not wish to speak with law enforcement. At this point, the officers did not interview her. Later, however, Win returned to law enforcement with her lawyer (and approval of this court by execution of a CJA travel voucher) and signed a consent form in the presence of counsel that allowed police to search all her electronic devices. Indeed, Win's attorney signed the consent form as a witness.

Agreeing to cooperate with a law enforcement investigation on advice of counsel is not coercive. Consent is voluntary if it is "the product of an essentially free and unconstrained choice by its maker." *United States v. Chaidez*, 906 F.2d 377, 380–81 (citing *Schneckloth v. Bustamonte*, 412 U.S. 218, 225 (1973)). The determination depends upon the totality of the circumstances in a particular case, including the characteristics of the accused and the details of the interrogation. Here, Win consented to the search. She does not allege that she was threatened, physically intimidated, or punished before she gave consent. Moreover, Win does not claim that she relied upon any promises or misrepresentations. The government has found no case law finding consent involuntary when the defendant, in the presence of and under the advice and consent of her counsel, consents to the search of property and executes such consent in writing. As such, the

defendant's motion to suppress should be denied.⁵

Dated: August 8, 2018

Respectfully Submitted,

ERICA H. MacDONALD
United States Attorney

s/Laura M. Provinzino
BY: LAURA M. PROVINZINO
Assistant United States Attorney
Attorney ID No. 0329691

MELINDA A. WILLIAMS
Assistant United States Attorney
Attorney ID No. 491005DC

United States Attorney's Office
300 South Fourth Street, Suite 600
Minneapolis, MN 55415
Telephone: 612-664-5600

⁵ Given the unambiguous nature of the defendant's consent to search her digital media, other than submitting the signed form as an exhibit, the United States will not be calling any witnesses on this suppression issue at the motions hearing.